

## Transnational Law and Criminal Justice System: Highlighting Legislative and Procedural Challenges to Combat Cyber Crime in the Wake of CPEC

Rana Saifullah<sup>1\*</sup> and Sayeda Sassi R. Shah<sup>2</sup>

1-PhD Candidate, Department of international relations, University of Karachi, Karachi, Sindh, Pakistan

2-Law student, University of London

\*Corresponding Author: [r\\_saifullah@hotmail.com](mailto:r_saifullah@hotmail.com)

### ABSTRACT

World Justice Project's (WJP) Rule of Law Index 2022 ranked Pakistan globally at 129<sup>th</sup> out of 140 countries while on regional level Pakistan is ranked 5<sup>th</sup> out of 6 countries. Where Pakistan's justice system is hitting the bottom in rule-of-law index, at the same time, the entire nation is celebrating China-Pakistan Economic Corridor (CPEC), which is a flagship project of Belt and Road Initiative (BRI) also known as OBOR. This is a Chinese master stroke in the cross-continental geo-economics of the world. With a heavy influx of Chinese businesses and Chinese nationals arriving in the country, the markets and Pakistani citizens are vulnerable to criminal activities including more sophisticated types of crimes such as crimes involving ICT. In particular, incidents of ATM skimming are rising in Karachi among other crimes. Foreign nationals are arrested include Chinese nationals; however, legislative and procedural lacunas and prosecution related defects eventually cause the prosecution version to collapse during trial. Therefore, this research study proposes strong legislative and judicial framework, human resource development including need for prompt initiatives in the subordinate judiciary. This research also highlights the need for having proper compliance of environmental and labor laws regulations. The research is based on mixed methodology. Quantitative analysis is conducted on the data collected through questionnaires from the sample of 50 respondents that include advocates, FIA investigation officers and public prosecutors. In addition, qualitative analysis is done through interviews of senior officers from NR3C as well as I.Os, students, academics and research economists from academia.

Article Type: Review Article

OPEN ACCESS



Copyright © 2023 The Authors

Received:  
20 March, 2023

Revised:  
5 June, 2024

Accepted:  
5 December, 2023

Published:  
20 December, 2023

**Keywords:** World Justice Project, Cybercrime, CPEC, ICT, Investigation, Prosecution, NR3C

**How to cite this article (APA):** Saifullah, R., & R. Shah, S. S. (2023). Transnational Law and Criminal Justice System: Highlighting Legislative and Procedural Challenges to Combat Cyber Crime in the Wake of CPEC. *JISR management and social sciences & economics*, 21 (4), 73-92.

<https://doi.org/10.31384/jismsse/2023.21.4.5>

**TABLE OF CONTENTS**

Introduction.....	75
Literature Review.....	75
Research Methodology.....	80
Structure of Questionnaire.....	81
Findings and Interpretation of the Results.....	82
Quantitative Analysis.....	82
Descriptive Statistics.....	83
Correlations.....	81
Model Summary <sup>a</sup> .....	82
Model Summary <sup>b</sup> .....	82
Coefficients <sup>a</sup> .....	82
Residuals Statistics <sup>a</sup> .....	83
Charts.....	82-83
Qualitative Analysis.....	83
Descriptive Statistics.....	84
Findings, Discussions and Suggestions.....	83
Policy Proposals and Recommendations.....	88
References.....	91

## INTRODUCTION

Chinese labors in Pakistan are prisoners sent to work on the CPEC. With prisoners coming in Pakistan for work purposes get themselves involved in crimes. Examples include hacking social media accounts and web portals, phishing, spamming, grey traffic, unauthorized radio operation, child pornography, cyber fraud and stalking, social media harassment, defamation and blackmailing. Cases of financial fraud including ATM skimming, unauthorized funds transfer, lottery scams and instant messaging applications like WhatsApp. This research aims to answer the following questions: What are the gaps in the judicial system of Sindh Subordinate Judiciary dealing with Chinese criminals? And what steps should be taken by (i) subordinate judiciary, (ii) law enforcement agencies, and (iii) legislation to deal with the problem? The primary goal of this paper is to explore the legislative and procedural lacunas that transform into the investigation and prosecution related defects that eventually cause the prosecution version to fall during trial. This paper proposes strong judicial, legislative and institutional framework as well as development of institutional work force.

## LITERATURE REVIEW

Crimes that are planned, carried out, or have an impact in more than one country are referred to as transnational crimes. The multinational dimension of these crimes distinguishes them from other types of criminal activity, providing particular issues in tracing their origins, developing prevention strategies, and adopting suitable adjudication procedures. The three broad categories of transnational crimes include the provision of illicit goods (drug trafficking, trafficking in stolen property, weapons trafficking, and counterfeiting), illicit services (commercial sex and human trafficking), and infiltration of businesses and government (fraud, racketeering, money laundering, and corruption) that affect multiple countries. International crime differs from transnational crime in that it covers crimes against humanity that may or may not include multiple countries.

Transnational organized crime has been defined in a study named judicial and social conditions for containment of organized crimes ([Buscaglia, 2021](#)). This study has discussed best judicial and civil society practices to prevent and combat organized crime. Organized crime is linked with serious and complex predatory crimes, such as human and organ trafficking and many other types of economic crimes (arms trafficking, gambling, smuggling and cyber-crime). It has not only allowed serious economic crimes but support for acts of terrorism as well, which is a threat to international human security. Lack of political strength, social dysfunction and lack of international coordination between states shaped

corruption and transnational organized crime. Corruption and organized crime is much more than a behavioral phenomenon linked to criminal law.

In a study, Balochistan caught in fragility trap disclosed a tentative but a notable shift in attitude of state towards conflict and criminality with significant new Chinese investment on horizon [Hasan \(2016\)](#). The lead security company named Frontier corps (FC) in Balochistan has been consistently accused of involvement in corruption and smuggling. Beyond FC, the National Accountability Bureau (NAB) in May 2016, has arrested Balochistan's finance secretary for corruption, recovering \$7.25 million. In 2015, investigations were begun against a senior police officer accused of myriad corrupt practices including smuggling of oil from Iran.

"One Belt, One Road" (OBOR) initiative is a step towards understanding the insight of the Asian century. OBOR is the plan's name that is formulated in order to restore and improve the soul of the old Silk Road. It comprises of different mega-projects, yet the fundamental two projects are "the Maritime Silk Road" (MSR) and the "Silk Road Economic Belt" (SREB), which were first unraveled to the world during the Chinese President Xi Jinping's visit to Indonesia and Kazakhstan in 2013. OBOR has a series of projects that connect the Baltic Sea with the Pacific Ocean by means of sea lanes, rails and roads for free trade. The OBOR has struck everyones concern as the sheer monstrosity of the endeavor proposes that it will be a distinct advantage for China, and all the stakeholders as well.

As referenced above, the OBOR is confronting huge examination in the West and as per reports of the New York Times in the wake of meeting government authorities in Washington DC, the Americans are attempting their best to abridge Chinas impact and this was apparent in their offer to assemble their partners against joining the AIIB, however they remained hopelessly unsuccessful in that endeavor, yet obviously they won't walk off-track from their China regulation policy. To seek after this end, they will utilize every one of the apparatuses available to them to either disrupt China strategically or contain it, through secretive methods. India being a nearby ally of USA for various years is being fortified as a component of their China regulation policy in the game of power struggle among China and USA in Asia. India, previously having its own territorial domineering plans and discord with China, thus creates an ideal option for USA as a partner in the area. With India raising hurdles among China and its fantasy of building up the OBOR regardless of being a component of the OBOR, just strengthens Western facilitation and Western pressures. Since by enhancing the region's economy could debilitate the main driver of terrorism and help balance out Central Asia and the Middle East, USA ought to be progressively positive about the enterprise as a settling power for basic good in the locale. The OBOR has been seen by Chinese organizers and their supporters as a distinct

advantage for the whole area. While the CPEC will be a forerunner of financial well-being and prosperity for Pakistan, China and the neighboring states. The two ventures will work with exchange organization, reinforced military union, and monetary thriving. Be that as it may, with expanded suspicion over the OBOR by USA and India's reservations concerning the CPEC, Pakistan needs to step cautiously and skillfully ([Moiz et al., 2015](#)). The Belt and Road Initiative (BRI) is creating physical connections among the regions attached to the project. The aim of BRI is also to establish the world's biggest platform for economic, trade, finance, social, cultural and policy cooperation. The state council China approved this plan in 2015. BRI consisted of two parts; Silk Road Economic Belt is a first part and the second one is 21 centuries Maritime Silk Road. The Maritime Silk Road projects will link the continents from South Asia to East Africa, and Europe to East Asia through the oceans and also will touch the Western pacific to the Mediterranean Sea and the Indian Ocean routs. There are many ports but they have less of a capacity for greater trade. China have hegemonic designs of BRI framework, many projects are facing problems in Chinese neighbor countries in Western pacific, specially seeking defense agreement with USA and Japan for recreation of peaceful relations. Gwadar port of Pakistan is contributing to faster and secure transportation of oil from Middle East to China, through shorter routes and stay away from the state of Malacca, in South Chinese Ocean. China will also take turn in safe access to Gwadar through its own borders. At present, transportation has required 45 days from Middle East to reach the Strait of Malacca. Through Gwadar port it could be reduced to minimum 10 days. The regional integration is an expected measure to see the demands of economically globalized world, the idea of Silk Road was rephrased by China in 2013 under BRI i.e., Economic Belt along the Silk Road and the 21 century Maritime Silk Road. As indicated by the joint paper, OBOR is an aftereffect of moderated development in the World economy, uneven worldwide advancement, and money related emergencies. The BRI is creating and increasing the opportunities for trade and investment in the BRI countries which have been attached with this mega project. As the other sectors are cooperating with each other to make it beneficial for this Belt and Road initiative, as well as the law sectors of these countries have also cooperated with each other to overcome the cross border legal issues and legal problems faced by the foreigner enterprises in their countries. There are different laws and legal rules about foreign trade and investment in the Belt and Road countries which may create problems for the foreign investors and enterprisers. So that the law cooperation among the Belt and Road countries having a great necessity of time. According to the article, Zhang Yan 23rd June 2017 in China daily, he described in the article that the legal professionals from China and the countries which have been attached with this Belt and Road initiative, have jointly released

an investment related laws guidebook. The purpose of this handbook is to prevent, help and provide solution of rising commercial disputes. It is said by a senior official of All China Lawyers Association (ACLA), the major law firms from the countries of Belt and Road will work jointly for the compilation of practical guidebook which will reduce the investment related risk when the enterprises make their investment in these countries. Another study proposes that, OBOR venture will be worldwide, including members from numerous nations. Choosing which law will oversee a task will be basic, not least to guarantee the fundability of the endeavor. Both business and political impacts likely could be in question and issues, for example, sureness of law and the speed/adequacy of an implementation system will be of significant contemplation. Likewise, various conflicts arise and the best discussion wherein to determine them is knowing about OBOR. Various jurisdictions are as of now trying to set up themselves as the 'go-to' place for OBOR dispute resolution. In more extensive impact, the legal difficulties to OBOR don't stop at foundation. A worldwide task requires a worldwide methodology and experience has demonstrated that harmonization of framework additionally requires harmonization of universal motivation. A venture of this scale is about something beyond setting up building blocks in place. OBOR's prosperity will require a more extensive arrangement of guidelines and legal standards, in a more extensive sense, where rights held in high respect in certain wards should likewise be fit to expel boundaries to advance, [Global Railway Review \(2018\)](#). As for criminal law in particular cybercrime and other criminal activities in which Chinese nationals are involved, [Mateen and Abbas \(2016\)](#) in their study titled as "Tsunami of Cybercrime: Analysis of Cybercrime New Trends, Causes and Remedies in Future Prospectus", has highlighted that People are not conscious of the actual use of technology. This Lack of awareness gives birth to new cyber-crime. Another study conducted by [Mohiuddin \(2006\)](#), titled as "Cyber laws in Pakistan: A situational analysis and way forward", has concluded that it is not possible to eliminate cybercrime but it is easier for Pakistan to tackle the issue and reduce it to large extend. Council of Europe's Convention on Cybercrime 2001 can help in forming better laws. [Saboohi \(2014\)](#) in a study titled as "Collecting digital evidence of cybercrime" has concluded that Evidence collection and experts in cyber technology are weak in Pakistan. In another study, it has been discussed that OBOR has included nations in Asia, Africa, and Europe. The points are to advance deliberate and free progression of financial elements, a very productive portion of assets and profound incorporation of business sectors. It goes for urging the inferred nations to "accomplish monetary arrangement coordination and complete more extensive and more inside and out local participation of higher gauges; and together making an open, comprehensive and adjusted provincial financial collaboration design that benefits all."

Today's period is the era of data and a decade from now there will be an era of data money. But this success of technology is directly proportional to cybercrime. Because a new app is created every day, as well as a new approach to break that specific conduct, the diversified nature of cybercrime makes investigation tough for different agencies. Sophistication is being attained in technical progress, and because cybercrime and technology are inextricably linked, there is still a long way to go in combating it. With the evolution of technology comes the discovery of new ways to tamper with and hack into it. Countries like China, United States of America, England, France, Japan, Korea etc. are considered to be the top digital and information technology hubs, but still due to cyber-criminal activities, the above mentioned countries have to face serious trouble and damage resulting in billions and billions of dollars. Any organization or corporation cannot implement a system or software capable of combating all cyber criminals and their cybercriminal activities. Is it possible to put a stop to cybercrime? The answer is "no," because it can only be confined to a certain area.

Pakistan is becoming increasingly concerned about cybersecurity. In recent years, the country has been subjected to several cyberattacks by both state and non-state adversaries. Cyber-espionage is a natural target for Pakistan's nuclear assets and crucial military locations. Projects like the China-Pakistan Economic Corridor (CPEC) are likewise vulnerable. India and its allied anti-Pakistan organizations continue to target Pakistan's defence facilities in the northwest and Balochistan. Evidence suggests that Indian intelligence is participating in attacks on Pakistan's media and communication networks with the goal of generating instability and fragmentation. Private hackers and professional criminals from all over the world, on the other hand, attempt to infiltrate Pakistan's cyberspace in order to steal data and information.

In terms of cyberattacks, 2018 was a perilous year for Pakistan. According to the Federal Investigation Agency (FIA), practically every bank in Pakistan has been subjected to a cyberattack. According to a PakCERT assessment, approximately 20,000 ATM card numbers were stolen and sold on the dark web. Due to development initiatives and cooperative businesses under the China-Pakistan Economic Corridor, Pakistan has seen a tremendous growth in Chinese nationals on its soil in recent years (CPEC). However, some Chinese expats have been caught up in illicit activities such as fighting and fraud. When a Chinese national was caught inebriated, he was sent to the hospital and then returned once he had sobered up. A Pakistani law enforcement agency arrested two Chinese citizens in March for ATM skimming fraud. The most recent cyber-attack on financial data occurred in Pakistan, with many people losing millions of rupees due to internet money transfers from one account to another.

In the same year, the Pakistan Air Force was subjected to a frightening cyber-attack. It was codenamed Operation Shaheen, and it involved the use of phishing techniques to obtain sensitive papers from the Air Force. In 2019, Rattlesnake, an international organization, attempted a similar attack on Pakistan's Naval Public Relations Bureau for stealing important information. In addition, some Pakistani high-ranking officials claimed that their Mobile Phones had been hacked for surveillance purposes.

Online stalking, cyber harassment, spoofing, spamming, extortion, kidnapping, and terrorism are all major issues in Pakistan. The government passed the "Prevention of Electronic Crime Act" in 2016. It was extremely beneficial to the Federal Investigation Agency (FIA). However, there are still numerous faults. The problem persists in the absence of a cybercrime policy, proper investigation methodologies, cutting-edge technologies, and professionals in computer and digital forensics. It is unavoidable that academia, experts, and the military have a role in countering cybercrime. However, a balance must be struck between cyber security and citizens' fundamental rights. If the former infringes on the latter, it will fail. Such issues must be addressed as soon as possible. Getting rid of such issues isn't a difficult undertaking. The digital world is changing at a breakneck pace. All of the industrialized countries' modern economies, education systems, and other systems are built on information technology and advanced digital technologies. Pakistan is still in the process of developing and is catching up to the rest of the globe. They are a century ahead of us due to their technology. We must pay special attention to our IT industry in order to compete with the modern developed world. So that we can compete with first-world countries, the government must establish a faultless policy on cybercrime, the digital world, and information technology.

## RESEARCH METHODOLOGY

The research methodology used for this study is a mixed approach. Primary technique of data collection is used to collect responses through questionnaires from 50 practicing advocates from sub-ordinate courts till the Supreme Court. Their standing at the bar ranges from two years to 50 years. This also includes a few lawyers who are handling cases of Chinese citizens involved in criminal activities. In order to achieve reliability and to cross validate the data, interviews are also conducted from the relevant individuals concerning law enforcement agency- F.I.A, academia, institutions as well as legal fraternity. In addition to that, one focus group discussion was also conducted which included participants from FIA, police and customs department and one advocate dealing appearing on behalf of Chinese nationals in criminal cases. This research study being a primary research is comprised of a questionnaires and interviews. Questionnaires are

based on Likert scale. The technique of sampling employed in this investigation is a convenience technique of sampling. Convenience technique of sampling is one of the sampling techniques of probabilistic where respondents are designated on the foundation of the well-known population. The utilization of simple random sampling mode delivers the prospect to choose respondents who are certainly available to the investigator.

### **Structure of Questionnaire**

The statistics are organized by source of a self-administered questionnaire which was constructed on a 5-point Likert scale from strongly disagree (1) to strongly agree (5). Data collected through questionnaires from the sample of 50 respondents. The purpose of validation of a self-administered questionnaire was done by the advocates, FIA investigation officers and public prosecutors. The questionnaire was adapted from past studies. This study uses the SPSS to obtain descriptive statistics, multiple regression and correlation generalized method of movement to investigate and thereafter, explains each investigate under separate headings.

## FINDINGS AND INTERPRETATION OF THE RESULTS

### Quantitative Analysis

Descriptive Statistics			
	Mean	Std. Deviation	N
CFGCC	4.7451	.43934	50
DIPT	4.6716	.47767	50

Correlations			
Pearson Correlation	CFGCC	1.000	.943
	DIPT	.943	1.000
Sig. (1-tailed)	CFGCC	.	.000
	DIPT	.000	.
N	CFGCC	50	50
	DIPT	50	50

Model Summary <sup>a</sup>							
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics		
					R Square Change	F Change	df1
1	.943 <sup>a</sup>	.889	.886	.14819	.889	390.475	1

Model Summary <sup>b</sup>			
Model	Change Statistics		Durbin-Watson
	df2	Sig. F Change	
1	49 <sup>a</sup>	.000	1.190

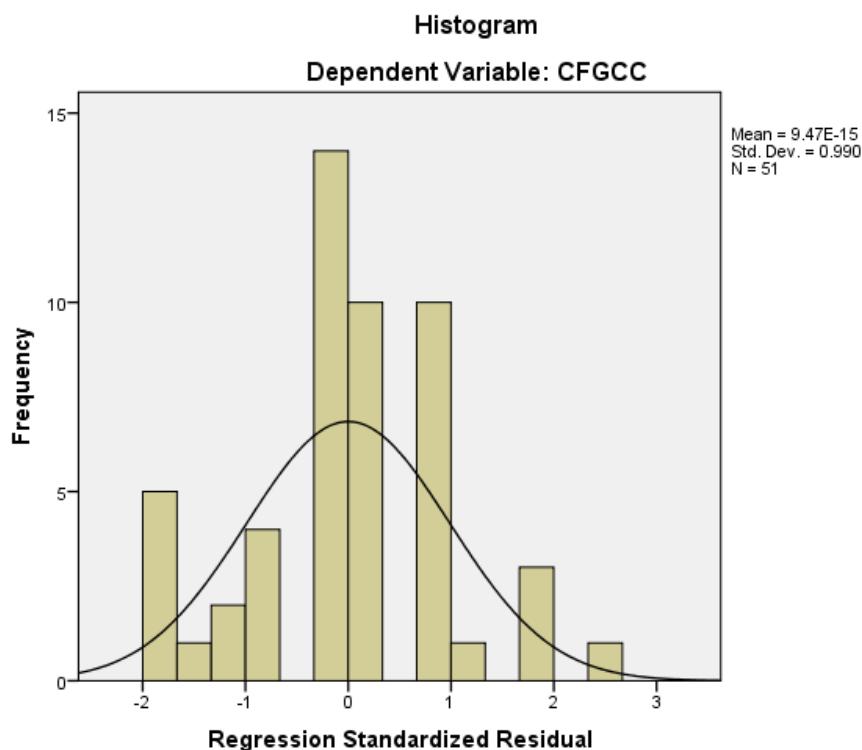
a. Predictors: (Constant), DIPT  
 b. Dependent Variable: CFGCC

Coefficients <sup>a</sup>						
Model	Unstandardized Coefficients		Standardized Coefficients		T	Sig.
	B	Std. Error	Beta			
(Constant)	.695	.206			3.374	.001
1 DIPT	.867	.044	.943		19.760	.000

### Charts

<b>Residuals Statistics <sup>a</sup></b>					
	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	3.5849	5.0298	4.7451	.41412	50
Residual	-.27722	.38026	.00000	.14670	50
Std. Predicted Value	-2.802	.688	.000	1.000	50
Std. Residual	-1.871	2.566	.000	.990	50

a. Dependent Variable: CFGCC



**Figure 1:**

## Qualitative Analysis

### Findings, Discussions and Suggestions:

There are four major wings around the country, each located in each province. 13 reporting centers are situated in major cities. There are around 13 investigation officers within Karachi which includes male and female both. Cybercrime has increased in the past two years. Around 13000 complaints are

filed in a year and only 13 I.O's are available to deal with them. Across Pakistan there are reported to be only 10 cybercrime experts to deal with such a major crime. Most complaints are classified as non-cognizable offences which present another challenge and a dent in prompt recovery and effective investigation. The instruments used in solving a crime related to electronic devices cost millions of rupees. It has been observed that the number of cybercrime complaints is already the highest than ever before and a shortage of investigation officers, trained prosecutors and required expertise of concerned judicial officers add severity to the problem. Pakistan deals with many social-media cyber issues as well. Issues such as Identity theft, cyber bullying, viral obscene pictures of girls by their ex-husband or any other related person to take revenge. To deal with this, FIA has to contact Facebook or Instagram headquarter to get these accounts removed. Pakistan does not have mutual legal assistance treaty (MLAT) with America which causes many problems in contacting such social media headquarters operated from San Francisco. This makes the procedure lengthy and difficult for FIA to handle and take control of. Social-media bullying also results in suicide of the victim, most cases are not reported because of societal pressure and family honor. Most of the time girls do complain but are reluctant to submit an FIR to police because they do not want their families to know of the matter. This results in acquittal of accused persons and fails to send out the message of deterrence to many offenders. Lack of forensic equipment's in many areas of Pakistan also results in weak forensic report which does not prove to be strong evidence in trial and does not back prosecution. Many offenders in Karachi are released on the basis of weak prosecution because of no proper forensic lab in Karachi or in major cities of Pakistan. Ethical hackers are found in most developed countries to tackle the issue of cybercrimes. In many cases when the information is needed to help in trial, it is unavailable, it is then those ethical hackers that hack into a computer system to gain information and provide it to government agencies for the benefit of society and victim. Pakistan does not have any institute to train and hire ethical hackers.

During interviews and focus group discussions, it has been transpired that most Chinese criminals are involved in cybercrime cases. The reason being there is no strict law and neither the strict compliance of law in Pakistan and these Chinese nationals know that we are a vulnerable nation. On top of that, the lack of knowledge among judicial officers about cybercrime and technical devices also add problems to the situation. In addition to that there is no proper scrutiny of documents at the Pakistani embassy in China. Had there been a proper check and deeper scrutiny of documents of the Chinese citizens coming to Pakistan, many people would be curtailed. The record suggests that most of the Chinese citizens involved in criminal activities arrive on business visa and many Chinese citizens come in greedy for money. They are not cyber experts

but they are too much into technology that it is easy for them to commit a crime. Their handlers are in Africa, Russia and China. Most of them are bank defaulters back in their home. Talking about the stance of Chinese embassy in Pakistan it does not support or endorse any criminal activity may it be an act of a Chinese citizen. Pakistani authorizes do contact Chinese embassy as well as concerned consulates after the arrest as well as conviction/ acquittal of the Chinese accused. Master minds are not being arrested and according to the respondent it is our law enforcement agencies who should be blamed, mainly due to corruption. Even the recovery from an arrested individual is usually understated. Interestingly the involvement of Pakistani law enforcement agencies cannot be ruled out from the commission of an offense as usually multiple persons are seen in CCTV at the ATM but only one is arrested. The respondent has stressed that investigation by FIA is weak and FIA should not feel any shame to induct investigation officers from police while the investigation by law enforcement must be separated from operations. Visa policy after CPEC is relaxed and it has become easier for Chinese nationals to come to Pakistan. The Chinese never use Pakistani ranks and now they have their own bank in Pakistan named Industrial and Commercial Bank of China Limited (ICBC). Chinese perform monetary transaction through WeChat and thereby they escape government taxes as there is no tax and no control of Pakistani law enforcement agencies on WeChat. As far as the judiciary is concerned, the jurisdiction of cybercrime is only vested with one judicial magistrate and a session's judge which has become a cause of delayed justice in likely cases. Most cases of Chinese in civil litigation pertains to registration of companies, rent cases, NOC related matters as well as marriage disputes. Another respondent expressed her concerns that CPEC is a flagship project of China and how do we ascertain whether it's a game changer or not especially when all the details are classified? The respondent expressed her concerns that we are unaware of how much they are earning in Pakistan and how much property they are buying while so much economic benefits are given to them. Other than that another major concern is a displacement of people from Gwadar and the Chinese are not respecting our labour laws either. The respondent has stressed that there must be some mechanism to deal with labour and environmental rights and civil society must come forward in this regard. We are being isolated at the foreign policy front and needed the ally and hence compromised on our own interests. She expressed further concerns with respect to the cultural aspect with hundreds and thousands of Chinese citizens coming to Pakistan. Another respondent, dean of management sciences at a reputed university and professor of human resource management also expressed his concerns whether it is right that the Chinese labour class is coming to Pakistan? There is a need for mutual legislation with respect to human resources. It is questionable as

to what percentage or ratio will be given to the Pakistani labour workforce as compared to Chinese citizens being employed in Pakistan. The main issue with respect to the human resource is the fact that their skill level is again to be decided by the Chinese companies as per their own job description. Chinese organizations and companies say that Pakistani workforce is not a competitive one. And that is how they find a reason to bring in their own workforce. During focus group discussion, the participants have unanimously agreed that even if we talk about Karachi alone, it is correct to suggest that crime rate has increased post CPEC and it is also correct that sophisticated crimes involving technology has reached its new heights with Chinese citizens involved in these offences. Chinese government are sending their prisoners to Pakistan and most of the laborers coming to Pakistan are themselves being disowned in their country and home. They are already into many kinds of criminal activities. May it be prostitution, kidnapping for ransom or any other criminal activity in the world, Chinese criminals are the first choice for any contract job even abroad. Even in European countries they are designated killers. They basically operate through gift shops. 90% of the laborers in KANUPP and Neelum Jehlum projects are Chinese citizens. One of the participants also stated that government of Pakistan cannot do anything and Chinese will never disclose any document which is likely to be disclosed to United States indirectly. No question arises as to whether we have bargained less or more or have we not bargained at all. We happily agreed on their terms. We must explore our own reserves of natural resources and rely on our own potential. Another aspect of the problem is that the classified documents and all the details without having details being made public, we cannot say anything, in-fact those documents being classified add ambiguity to the integrity of the mega project. We have been sending delegations to China but it has been observed their almost 90% of the participants or delegates are not relevant to the visits to China. After the Sri Lankan port has gone in the hands of China and the way it happened, has certainly made the situation alarming for all of us as a nation.

The supervisor of this research has rich experience of Chinese socio-economic and political dynamics and has stressed that the problem being highlighted in this study is a cogent one and needs to be tackled on an immediate basis. It is correct that many Chinese citizens are coming into Pakistan in the wake of CPEC and certainly there are many cases already being reported in which Chinese citizens are involved. As far as corporate governance and economy is concerned, heavy investment is coming to Pakistan and CPEC is only assumed to be just a corridor whereas CPEC is much more than just a corridor. Chinese are secretive in their dealings and when things are not public, it casts shadows on transparency and threatens the corporate governance as well as the integrity of the projects. There is no check and balance on trade through CPEC and no checks

on the businesses working in Pakistan. This calls for indigenous steps to be taken in code of corporate governance to ensure transparency and accountability of these firms. In China, there is no Google, no WhatsApp and all communications and surfing is through their own domains and WeChat and everything is mostly secretive to their citizens but monitored by Chinas state government for the use of proxy. It is alarming that China is shifting its polluted industries to Pakistan and we need to keep a check on the industry they are bringing in. As for shareholding, they are increasing their shares in power sector and we know that they are operating K-Electric already in Karachi. Their ownership is not controlled neither monitored. While the entire focus of the Pakistani government and the nation is towards the revenue generation without realizing the cost. It is suggested that one of the directors of the companies operating in Pakistan must be a Pakistani citizen and Chinese businesses should be brought under the tax net. CPEC would only be a game changer only and only if the terms are settled on a 50-50 basis. China is saving a lot of distance and thus cost of production through CPEC. All big deals are classified and are not being disclosed. Answering to a question about WeChat, he disclosed that transactions through WeChat can be used for negative and criminal purposes as well as to avoid tax.

## POLICY PROPOSALS & RECOMMENDATIONS

With globalization taking over Pakistan, it is important for cybercrime experts to learn to deal with international criminals. It is being proposed that it is necessary to impart skill based training to investigating officers and prosecutors besides increasing their employment in the public sector. Sensitizing learned judicial officers with the help of exchange training programmers and giving required exposure to deal with such crimes and maintaining the sensitivity of cases relating to child pornography in particular - Kasur child pornography case. It has been observed that the number of cybercrime complaints is already at the highest than ever before and shortage of investigation officers, trained prosecutors and judicial officers add severity to the problem. Strong legislative and institutional framework, development of institutional work force development to tackle all possible kinds of cyber-attacks. As it has been discussed that China and Pakistan are collaborating in building bridges and roads they should also collaborate in dealing with cybercrime as in China cybercrime mafia is increasing day by day. Therefore, a separate agency should be formed to deal with cross border crimes for effective and timely action. In Pakistan INTERPOL is controlled by FIA. But as China and Pakistan are developing stronger bonds it is important for both countries to have their own agency to deal with such issues for prompt and effect. It is necessary for NADRA to access all information about each Chinese or international worker coming into Pakistan, the information should be easily accessible and consist of all past activities of that person. MLAT needs to be signed with foreign countries where social media headquarters are located. Otherwise Pakistan needs to ban international social media applications and invent their own like China did. Weibo, WeChat, Youku and more are the main social media channels in China. The reason behind this is that China doesn't need to contact international social media networks to gain information of cyber related activity but they can gain information from their own local companies without MLAT and special permission from courts. Forensic labs should be formed near each NR3C wing to help with better investigation. It has been reported that due to the lack of a forensic report or delay in a forensic report the offender escapes the conviction which does not result in deterrence. Ethical hackers are needed in Pakistan to work with government agencies to control cybercrime. With recruiting ethical hackers in agencies, the job will become much easier to handle. Special schools should be set up to provide technical training in learning ethical hacking, its limits and importance in the world of law. Special courts are needed to deal with cybercrime where the judges should be computer experts or have information about computer sciences which can help them understand the investigation procedure. Judges should also be trained in dealing with variety of case related to electronic devices. Along with this investigation officers are needed to be

trained every year and provided with advance technology to solve the crimes. Training sessions with international experts and collaboration with successful investigation agencies will help in increasing the efficiency and technical skills of local I.O's. For effective solution of civil dispute, there needs to be in place a proper arbitration centers whereas the commercial disputes dealing under capital ICSID are already high cost. It is hence suggested that the jurisdiction of the cybercrime cases should be vested with multiple judicial officers including ADJs who should be given cybercrime cases to try other than a session's judge. Arbitration can be a solution to address civil cases but for that we must train our judicial officers or expert mediator or arbitrator. Besides that, it is inevitable to have special courts dealing with the cases of cybercrime to lessen the burden on the existing judicial system. In addition to that, we do not have any treaty with China with respect to jurisdiction which makes this situation more complex. Media should play a positive role or at least a neutral role because even Pakistani citizens have committed fraud with Chinese nationals and their rights should also be safeguarded. Furthermore to safeguard labour rights and interests of our own workforce, it is also suggested that there is a need to have decentralized government board working at the federal level and its decentralized branches at the provincial level to oversee employment while its TORs and SOPs are to be settled by the board. TEVTA has to come on front foot to play its role in developing the human resource and to create skilled labour for the projects. From last few years NAVTEC is not as effective as before therefore we have to rely on TEVTA for the preparation of skilled labour. Pakistani universities should prepare students for the required employment and to deal with Chinese businesses and other citizens in their daily life. As far as laws are concerned, we need effective implementation and due compliance of our labour laws besides redefining criminal laws to combat the volume of litigation as well as to protect our interests. At this stage, we cannot ignore the environmental aspect attached to CPEC as well and need to safeguard our environment effectively, besides safeguarding our other basic and fundamental interests. Furthermore, training of judicial officers and other court staff is also necessary as the volume of litigation is expected to rise. There is no competitive education of law. Law should be made a compulsory course in every subject as it gives due awareness of a persons fundamental rights. There is a need to have mutual consultancy between the two countries at the state level as China primarily deals with states. However, as far as Chinese investment and Chinese citizens coming to Pakistan is concerned, interior ministry is required to put proper controls and check at the entry point. And to deal with the issue of employment, Pakistan should raise the level of its Human Resource competitiveness. Joint dispute resolution mechanisms should be deployed. There has to be an element of transparency and things should be made public. They should be put to public scrutiny.

Also, there is a need to change our policies and the Chinese businessmen in Pakistan should be brought under tax net. There is a need of having concrete legislation and need for policy formulation at the same time, labour laws should be well protected and complied with and we need to protect our labour class and safeguard their rights. Proper environmental regime is required on an immediate basis and the Ministry of Environment must scrutinize the entry of Chinese businesses and industries coming to Pakistan that are likely to pose a serious threat to the environment. It has been also disclosed that China is embarking upon having one currency for the entire OBOR. They have already established their ICBC bank in Karachi where there are transactions charges are way less while they can make payments and perform monetary transfers through their own banks.

## REFERENCES

A brilliant plan One Belt, One Road. (2015). *CLSA*. Retrieved from <https://www.clsacom/special/onebeltoneroad>

Abid, M., & Ashfaq, A. (2015). CPEC: Challenges and opportunities for Pakistan. *Journal of Pakistan Vision*, 16(2), 142–169.

Ali, M., & Li Lu Geng. (2018). Legal Cooperation in Perspective of Belt and Road Initiative and China Pakistan Economic Corridor. *International Journal of Research*.

Arrfat, Y. (2018). *Challenges & solutions in building CPEC-A Flagship of BRI*.

Buscaglia, E. (2021). Judicial and Social Conditions for the Containment of Organized Crime: A Best Practice Account. In Heinrich-Böll-Stiftung & R. Schönenberg (Eds.), *Transnational Organized Crime: Analyses of a Global Challenge to Democracy* (pp. 61–74). Bielefeld: Transcript Verlag. <https://doi.org/10.1515/transcript.9783839424957.61>

Catanza, J., Qi, R., Jia, C., & Shan, B. (2015). *Silk Road initiative connects countries on path of prosperity*. *The Telegraph*, 3 July 2015. 13. Chowdhury, D. Roy. (Nov. 19, 2013). "Pakistan happy to aid in China's quest for land route to the west; India, not so much." *SouthChina Morning*.

Giacobozzi, K. (2011). *Cyber-Terrorism*.

Global Railway Review. (2018).

Hasan, A. (2016). *US Institute of Peace*. Retrieved June 28, 2021.

Hussain, E., & Rao, M. F. (2020). China-Pakistan Economic Cooperation: The Case of Special Economic Zones (SEZs). *Fudan J. Hum. Soc. Sci*, 13, 453–472. <https://doi.org/10.1007/s40647-020-00292-5>

Jibran, F. (2021). Cybersecurity in Pakistan: A Grave Vulnerability | Paradigm Shift. Retrieved 28 June 2021.

Jinchen, T. (2016). *One Belt and One Road": Connecting China and the world* | McKinsey & Company. Retrieved from <https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/one-belt-and-one-road-connecting-china-and-the-world>

Liping, X. (2015). *The Development of the "One Belt and One Road" and its Impact on China-US Relations*. Chinese People's Association for Peace and Disarmament. Beijing, China. 6. Catanza, Joseph. Qi, Ren. Jia, Chen. & Shan, Bu. (2015, July 3). *Silk Road Initiative connects countries on path of prosperity*. *The Telegraph*.

Malik, A. R. (2018). *CPEC's legal dimension published in The Nation*.

Mateen, A., & Abbas, Q. (2016). *Tsunami of Cybercrime: Analysis of Cybercrime New Trends, Causes and Remedies in Future Prospectus*. <https://doi.org/10.5120/ijca2016911909>

Mohiuddin, Z. (2006). *Cyber laws in Pakistan: A situational analysis and way forward*.

Moiz, H. S., et al. (2015). *One Belt and One Road: Impact on China-Pakistan Economic Corridor*.

Rai, R. (2013). Cybercrimes- Challenges & Solutions. *International Journal of Computer Science and Information Technologies*, 4(5), 729–732.

Saboohi, M. (2014). *Collecting digital evidence of cybercrime*.

Ullah, S. (2015). *Pakistan and Cybercrimes: Problems and Preventions*. <https://doi.org/10.1109/Anti-Cybercrime.2015.7351951>